

## Warranty

Corega International warrants product for two years from date of purchase against defects in materials and workmanship. This warranty does not cover any defects caused by accident, misuse, fair wear and tear, neglect, or an attempt at repair. This warranty is offered as an additional benefit to the consumer's statutory rights and does not affect these rights in any way.

Corega International shall not be held responsible for any special, incidental, or consequential damages resulting from any breach of warranty, or under any other legal theory, including but not limited to lost profit, downtime, damage to data stored in or used with Corega International products.

## Trademarks

Corega™ is a trademark of Corega Holdings KK., Japan.

Other trademarks, brand and product names are acknowledged as trademarks of their respective holders. Information is subject to change without notice.

All rights reserved.

## (GB) Warnings

### ELECTRIC SHOCK HAZARD:

Install product in accordance with local and National Electrical Codes.

To de-energise equipment, disconnect the power cord.

## (D) Warnhinweise

### STROMSCHLAGGEFAHR:

Dieses Produkt muss entsprechend den örtlichen und nationalen Elektrizitätsvorschriften installiert werden. Zum Abschalten der Ausrüstung Stromkabel abziehen.

## (I) Attenzione

### RISCHIO DI SHOCK ELETTRICO:

Installare l'apparecchio in base alle normative elettriche locali e nazionali. Per togliere l'alimentazione al dispositivo, scollegare il cavo relativo.

## (E) Advertencias

### PELIGRO DE ELECTROCUCIÓN:

Instale el producto de acuerdo con las recomendaciones de la normativa sobre instalaciones eléctricas de su país. Para desactivar el equipo, desconecte el cable de alimentación.

## (F) Avertissements

### RISQUE D'ÉLECTROCUTION:

Installez le produit conformément aux réglementations électriques nationales et locales. Pour mettre l'équipement hors tension, débranchez le cordon d'alimentation.

## (FIN) Varoitukset

### SÄHKÖISKUN VAARA:

Asenna tuote noudattaen paikallisia ja kansallisia säädöksiä. Laitteen saa jännitteettömäksi vain irroittamalla sähköjohto.

## (RUS) Предупреждения

### ОПАСНОСТЬ ПОРАЖЕНИЯ ЭЛЕКТРИЧЕСКИМ ТОКОМ:

Устанавливайте изделие в соответствии с местными и национальными правилами по установке электрооборудования. Для отключения питания отключите шнур питания.

Предупреждение – это изделие класса А. В домашних условиях это изделие может создавать радиопомехи. В этом случае пользователю, возможно, понадобится принять соответствующие меры.



# **ADSL WIRELESS 802.11g 54MBPS ROUTER**

**COR-WLBAR-AA & COR-WLBAR-AB  
ALL-IN-ONE-ROUTER**



[www.corega-international.com](http://www.corega-international.com)

## Table of Contents

|   |           |
|---|-----------|
| <b>FCC STATEMENT</b>  | <b>2</b>  |
| <b>CE DECLARATION OF CONFORMITY</b>                           | <b>2</b>  |
| <b>MANUFACTURER'S DISCLAIMER STATE</b>                        | <b>2</b>  |
| <b>CHAPTER 1.0: GETTING TO KNOW YOUR ADSL WIRELESS ROUTER</b> | <b>3</b>  |
| 1-1 FEATURES OF THE ADSL WIRELESS ROUTER                      | 3         |
| 1-2 CONTENTS OF THE ADSL WIRELESS ROUTER PACKAGE              | 3         |
| <b>CHAPTER 2.0: HARDWARE INSTALLATION &amp; SETUP</b>         | <b>4</b>  |
| 2-1 CONNECTORS AND INDICATORS                                 | 4         |
| 2-2 INSTALLATION  | 5         |
| <b>CHAPTER 3.0: BASIC INSTALLATION &amp; SETUP</b>            | <b>6</b>  |
| 3-1 ONE PAGE SETUP  | 7         |
| 3-1-1 GATEWAY USING PPPoE                                     | 8         |
| 3-1-2 GATEWAY USING PPPoA                                     | 9         |
| 3-1-3 GATEWAY USING DYNAMIC IP                                | 9         |
| 3-1-4 GATEWAY USING STATIC IP                                 | 10        |
| 3-1-5 GATEWAY USING CLASSICAL IP                              | 10        |
| 3-1-6 MODEM USING LLC ENCAPS.                                 | 11        |
| 3-2 CONFIGURE WIRELESS SECURITY                               | 12        |
| 3-2-1 WEP ENCRYPTION  | 12        |
| 3-2-2 WPA-PSK ENCRYPTION                                      | 13        |
| 3-3 STATUS  | 14        |
| <b>CHAPTER 4.0: ADVANCED CONFIGURATION</b>                    | <b>15</b> |
| 4-1 DHCP CONFIGURATION  | 15        |
| 4-2 DMZ CONFIGURATION   | 16        |
| 4-3 FIREWALL RULES  | 17        |
| 4-4 FIREWALL SERVICES   | 18        |
| 4-5 INTERNET ACCESS CONTROL                                   | 19        |
| 4-5-1 INTERNET ACCESS CONTROL - URL FILTER SETTINGS           | 20        |
| 4-6 PORT FORWARDING (VIRTUAL SERVER) SETTINGS                 | 21        |
| 4-7 DDNS  | 22        |
| 4-8 SPECIAL APPLICATIONS                                      | 23        |
| 4-9 MISCELLANEOUS OPTIONS                                     | 24        |
| 4-10 ROUTING  | 25        |
| 4-11 TIME SCHEDULE  | 26        |
| 4-12 WIRELESS ACCESS CONTROL                                  | 27        |
| 4-13 VPN CONFIGURATION  | 28        |
| 4-13-1 VPN - ADD MANUAL POLICY                                | 29        |
| 4-13-2 VPN - ADD AUTO POLICY                                  | 31        |
| <b>CHAPTER 5.0: MANAGEMENT</b>                                | <b>33</b> |
| 5-1 PC DATABASE   | 33        |
| 5-1-1 PC DATABASE - ADVANCED ADMINISTRATION                   | 34        |
| 5-2 PASSWORD  | 35        |
| 5-3 REMOTE ACCESS   | 36        |
| 5-4 NETWORK DIAGNOSTICS                                       | 37        |
| 5-5 LOG   | 38        |
| 5-6 EMAIL   | 39        |
| 5-7 CONFIG FILES  | 40        |
| 5-8 FIRMWARE UPGRADE  | 41        |
| <b>CHAPTER 6.0: TROUBLESHOOTING</b>                           | <b>41</b> |
| HARDWARE  | 41        |
| CLIENT SIDE (COMPUTERS)                                       | 42        |
| <b>APPENDIX A: FREQUENTLY ASKED QUESTIONS</b>                 | <b>43</b> |
| <b>APPENDIX B: TECHNICAL SPECIFICATIONS</b>                   | <b>44</b> |
| <b>APPENDIX C: GLOSSARY</b>                                   | <b>45</b> |

### **FCC Statement**

This device complies with Part 15 of FCC rule. Operation is subject to the following two conditions:

This device may not cause harmful interference.

This device must accept any interference received, including interference that may cause undesired operation.

This ADSL Wireless Router has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used according to the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which is found by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment or device.

Connect the equipment to an outlet other than the receiver's.

Consult a dealer or an experienced radio/TV technician for assistance.

### **FCC Radiation Exposure Statement**

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

### **CE Declaration of Conformity:**

This equipment complies with the specifications relating to electromagnetic compatibility, EN 55022/AT Class B, and EN 50082-1. This meets the reasonable protection requirements set out in the European Council Directive on the approximation of the laws of the member states relating to Electromagnetic Compatibility Directive (89/336/EEC).

### **Manufacturer's Disclaimer State**

The information in this document is subject to changes without notice and does not represent a commitment on the part of vendor. No warranty or representation, either expressed or implied, is made with respect to the quality, accuracy or fitness for any particular purpose of this document. The manufacturer reserves the right to make changes to the content of this document and/or the products associated with it at any time without obligation to notify any person or organization. In no event will the manufacturer be liable for direct, indirect, special, incidental or consequential damages arising out of the use or inability to use this product or documentation, even if advised of the possibility of such damages. This document contains materials protected by copyright. All rights are reserved. No part of this manual may be reproduced or transmitted in any form, by any means or for any purpose without the expressed written consent of its authors. Product names appearing in this document are mentioned for identification purchases only. All trademarks, product names or brand names appearing in this document are registered property of their respective owners.

## Chapter 1.0 Getting to know your ADSL Wireless Router

### 1-1 Features of the ADSL Wireless Router

Congratulations on your purchase of this ADSL Wireless Router.

The router provides the following benefits:

- High Speed internet Access over ADSL (Up to 8Mbps internet downstream speed and 832Kbps upstream speed).
- Allows multiple computers to share a single ISP internet account.
- Wireless LAN connection via integrated Wireless Access Point.
- Provides 64bits/128bits key WEP (Wired Equivalent Privacy) and WPA-PSK wireless data encryption to secure wireless communication.
- 4 port 10/100Mbps switch for wired connections to computers and printers.
- DHCP Server providing local IP addresses to local computers.
- Complete data security protecting the network from hackers.
- In-built filters allow denial of access to objectionable websites.
- Virtual Private Network support (VPN) and IPSec support.

### 1-2 Package Contents

After carefully unpacking the shipping carton, check the contents listed below.

- 1 x ADSL Wireless Router
- 1 x Power Adapter
- 1 x User's Manual
- 1 x Telephone Cable
- 1 x Ethernet Cable
- 1 x CD



Figure 1. Pack Contents

Chapter 2.0 Hardware Installation and Setup

2-1 Connectors and Indicators

The front and rear panels of the router are shown in Figure 2.

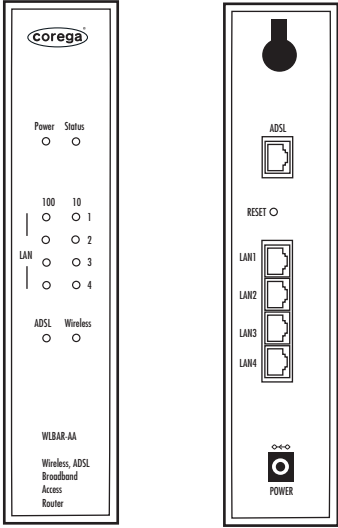


Figure 2. Front & Rear Panels.

Rear Panel Connectors

- Antenna
- Reset
- ADSL
- LAN 1—4
- Power

Provides data transmission and reception for wireless devices. Please ensure that the Antenna is facing upwards.  
Pressing this button for 3 seconds will reset the unit back to factory defaults.  
This is the WAN connection port to the telephone socket.  
Four LAN ports for local computers/printers.  
Inlet socket for external power adapter.

Front Panel Indicators

- Power
  - Off - No power applied
  - Green - Power to the router
- Status
  - Yellow - Glows when the router performs a self test, and diagnostics.
  - Off - When router is operating correctly.
- WLAN Enable/Activity
  - Off - Wireless not enabled
  - Green - Wireless enabled
  - Flashing - Data activity on the wireless port
- 10/100 LAN Link/Activity
  - Off - Port not active
  - Green - Port has valid connection
  - Flashing - Data activity on the port
- ADSL Link/Activity
  - Off - ADSL line not connected
  - Green - ADSL connection is established and ready
  - Flashing - ADSL connection is being established

## 2-2 Installation

Connect the router as shown.

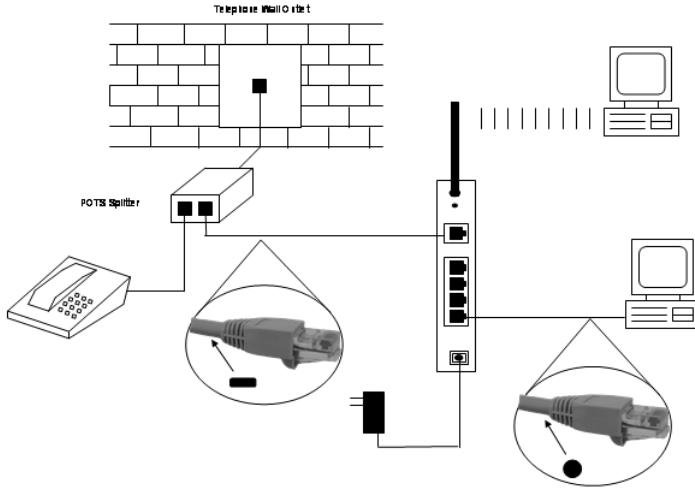


Figure 3. Hardware Installation

Power on the devices in the following sequence:

- ADSL Router
- Computer(s)

**Note!** The computer needs to be configured with the following:

- Ethernet Card supporting either;
  - 10Base-T
  - 100Base-TX
  - 802.11b or 802.11g Wireless
- TCP/IP Protocol
- Web browser such as Microsoft Internet Explorer 4.0 or later.

**Note!** If you are connecting via a wireless connection – the Access Point in the router is programmed with the following default parameters:

SSID - corega  
WEP - disabled

Chapter 3.0 Basic Installation & Setup

This chapter describes the procedures necessary to configure the basic functions of the router to allow internet access.  
The following information should be supplied by your ISP:

|                         |   |
|-------------------------|---|
| Provided by some ISPs   | Host Name:<br>Domain Name:  |
| IP address given by ISP | <ul style="list-style-type: none"><li>Dynamic</li><li>Static</li></ul> IP address<br>Subnet Mask<br>Default Gateway<br>DNS Server (Primary)<br>DNS Server (Secondary)   |
| WAN VPI and VCI Values  | VPI<br>VCI  |
| Operating Mode          | <ul style="list-style-type: none"><li>LLC Encapsulation with Dynamic IP</li><li>LLC Encapsulation with Static IP</li><li>Gateway Classical IP</li><li>PPPoE</li><li>PPPoA</li><li>Router using Classical IP</li></ul> |
| PPP Authentication      | Login Name<br>Password  |

Depending on your ISP, some or all of these parameters need to be programmed into the router.  
Before attempting to configure the router, Corega suggest that you visit the support site of [www.corega-international.com](http://www.corega-international.com), and download a configuration file which may help you with your particular installation. This should setup most of the parameters such that you only have to enter your username and password.  
To access the router, point your web browser at: **http://192.168.0.1**

**Note!** For most users, a compatible IP address will be automatically allocated to each computer by the router's internal DHCP server. If you cannot access the router – check that the computer has been set to receive a dynamic IP address or manually configure a compatible IP address.  
From Windows:  
Start/Settings/Network & Dial Up Connections/Local Area Connection/Properties/TCP/IP

The following screen should appear:



Figure 4. Login Screen

The factory default values are:  
Username        admin  
Password       password

Click **OK**.  
The following screen should appear:



### 3-1 One Page Setup

**corega**

**Main Menu**

- OnePage Setup
- Status

**Advanced Function**

- DHCP
- DMZ
- Firewall Rules
- Firewall Services
- Internet Access Control
- Port Forwarding
- Dynamic DNS
- Special Applications
- Miscellaneous Options
- Routing
- Schedule
- Wireless Access Control
- VPN

**Management**

- PC Database
- Password
- Remote Admin
- Diagnostics
- Logs
- E-mail
- Config File
- Upgrade Firmware

**One Page Setup**

**General**

Host Name:  (Required by some ISPs)

Domain Name:  (Required by some ISPs)

Private IP Address:  192  168  0  1

Subnet Mask:  255  255  255  0

Timezone:  (GMT) Greenwich Mean Time : Edinburgh, London

**Wireless**

SSID (Service Set Identifier)  corega

☒ Broadcast SSID Enable (default On)

Mode:  802.11g & 802.11b

Region:  Europe

Channel No:  03

Wireless Security (default Off): Disabled

**VC Settings**

VPI:  8 ( 0 ~ 255 )

VC:  35 ( 32 ~ 65535 )

Encapsulation:  VC-BASED

**WAN Connection**

Gateway using PPPoE (MAC: 00:c0:02:ee:45:e3)

Login Name:

Password:

☐ Connect on Demand: Max Idle time:  0 min

☒ Keep Alive: Redial Period:  60 sec

Figure 5. One Page Setup

By setting the parameters on this page, users should then be able to access the internet using the router.

#### General

- Host Name:** This entry is required by certain ISPs. (If not necessary – leave blank).
- Domain Name:** This entry is required by certain ISPs. (If not necessary – leave blank).
- Private IP Address:** This is the LAN IP address of the router. This is the address that is used to configure the router. The default values are:  
192.168.0.1 for IP Address and  
255.255.255.0 for Subnet Mask.

(Changing this factory default setting is optional, and is not necessary for most small networks).

- Time Zone:** Select the relevant time zone from the drop down list. (Setting this is optional)

#### Wireless

- SSID:** (Service Set Identifier). SSID is the unique name shared among all clients and the router in a wireless network. The SSID must be identical for all wireless devices and must not exceed 32 characters. The default value for the SSID is 'corega'.
- Broadcast SSID Enable:** The router will broadcast the SSID to let wireless clients easily search and connect to this router. Default value is "enabled".
- Mode:** The router can operate in three possible modes. Select from the drop-down menu one of the following:  
802.11g & 802.11b Allows the router to connect to 11Mbps (802.11b) and 54Mbps (802.11g) clients (Recommended)  
802.11g Allows the router to connect only to 54Mbps (802.11g) clients  
802.11b Allows the router to connect only to 11Mbps (802.11b) clients
- Region:** Select the appropriate region from the drop-down menu. The permissible channels are different in each country due to local government regulations.
- Channel:** Select the appropriate channel number from the drop-down menu. Make sure that all nodes in the same wireless LAN network use the same channel.
- Wireless Security Status:** This shows the status of the wireless security function. Default value is disabled. To enable, click on **Configure wireless security**.
- Configure Wireless Security:** See section. 3.2 on page 12.

### VC Setting:

- **VPI:** If you have uploaded a config file (see section 5.6 on page 39, this parameter will already be set. This is a value between 0-255 and is provided by your Internet Service Provider (ISP).
- **VCI:** If you have uploaded a config file, this parameter will already be set. This is a value between 32-65535 and is provided by your Internet Service Provider (ISP).
- **VPI,VCI Auto Detect:** If you have not uploaded a config file, and are not sure of the VPI and VCI parameters required by your ISP, then this utility will attempt to determine the correct VPI & VCI parameters by examining the ADSL interface. (Make sure that the router is connected to the ADSL line if you use Auto Detect.
- **Encapsulation:** If you have uploaded a config file, this parameter will already be set. This will be set as either LLC or VC based, and is provided by your Internet Service Provider (ISP).

### WAN Connection

If you have uploaded a config file (see section 5-6), this parameter will already be set. WAN Connection type is the way the router works with DSLAM equipped in your ISP side. This ADSL Wireless router supports six connection types listed as below. Different countries, and different operators use different types of connection type. It is important to select the correct type for your network provider. If you are unsure about which WAN Connection Type, please consult your provider.

- Gateway using PPPoE
- Gateway using PPPoA
- Gateway using Dynamic IP
- Gateway using Static IP
- Gateway using Classical IP (IP over ATM)
- Modem using LLC Encap

#### 3-1-1 Gateway using PPPoE

The screenshot shows the 'WAN Connection' configuration page. The title is 'WAN Connection'. Below it, a dropdown menu is set to 'Gateway using PPPoE', with the MAC address '00:c0:02:ee:45:e3' displayed next to it. There are input fields for 'Login Name:' and 'Password:'. Below these are three radio button options: 'Connect on Demand: Max Idle time: 0 min', 'Keep Alive: Redial Period: 60 sec' (which is selected), and 'Manual Connect/Disconnect'. Below these is the 'WAN IP Address:' section, with 'Automatic/Dynamic (Default)' selected. There is also an option for 'Fixed' IP address with four input boxes. At the bottom right are 'Save', 'Cancel', and 'Help' buttons.

Figure 6. Gateway using PPPoE

- **Login Name:** Enter your ISP Username.
- **Password:** Enter your ISP Password.
- **Connect-on-demand:** Only enable this option if your ISP charges by the megabyte or by minutes (seconds) of line usage. Enabling this option will cause the router to connect to the ADSL line when there is a packet waiting to be transmitted. Set the **Max Idle Time** with the length of time the router will remain in an idle state before reconnecting to collect incoming data.
- **Keep Alive:** This function keeps your PPPoE connection always active even when there is no data to transmit. However, in some situations, the PPPoE session cannot be built immediately after disconnection because the system on the ISP site may need a little time to restore. You may need to check with your ISP to find out how much time is required before the router can start to re-build the PPPoE session and then fill this in the "**Redial Period**".
- **Manual Connect/Disconnect:** Allows the user to manual connect or disconnect the ADSL connection from the keyboard.
- **IP Address:** This is the IP address of the WAN port. In most cases (default), this will be a **Dynamic** IP address. In some cases, this will be a **Static** IP address issued by your ISP. If this is the case, select Fixed, and enter the IP address.

### 3-1-2 Gateway using PPPoA

The screenshot shows the 'WAN Connection' configuration window. On the left is a grey sidebar with the text 'WAN Connection'. The main area has a dropdown menu set to 'Gateway using PPPoA' with '(MAC: 00:c0:02:ee:45:e3)' next to it. Below this are fields for 'Login Name:' and 'Password:'. There are three radio button options: 'Connect on Demand: Max Idle time: 0 min', 'Keep Alive: Redial Period: 60 sec' (which is selected), and 'Manual Connect/Disconnect'. Below these is the 'WAN IP Address:' section with 'Automatic/Dynamic (Default)' selected and 'Fixed:' with four empty boxes. At the bottom right are 'Save', 'Cancel', and 'Help' buttons.

Figure 7. Gateway using PPPoA

- **Login Name:** Enter your ISP Username.
- **Password:** Enter your ISP Password.
- **Connect-on-demand:** Only enable this option if your ISP charges by the megabyte or by minutes (seconds) of line usage. Enabling this option will cause the router to connect to the ADSL line when there is a packet waiting to be transmitted. Set the **Max Idle Time** with the length of time the router will remain in an idle state before reconnecting to collect incoming data.
- **Keep Alive:** This function keeps your PPPoE connection always active even when there is no data to transmit. However, in some situations, the PPPoE session cannot be built immediately after disconnection because the system on the ISP site may need a little time to restore. You may need to check with your ISP to find out how much time is required before the router can start to re-build the PPPoE session and then fill this in the "Redial Period".
- **Manual Connect/Disconnect:** Allows the user to manual connect or disconnect the ADSL connection from the keyboard.
- **IP Address:** This is the IP address of the WAN port. In most cases (default), this will be a **Dynamic** IP address. In some cases, this will be a **Static** IP address issued by your ISP. If this is the case, select Fixed, and enter the IP address.

### 3-1-3 Gateway using Dynamic IP

The screenshot shows the 'WAN Connection' configuration window. On the left is a grey sidebar with the text 'WAN Connection'. The main area has a dropdown menu set to 'Gateway using Dynamic IP' with '(MAC: 00:c0:02:ee:45:e3)' next to it. At the bottom right are 'Save', 'Cancel', and 'Help' buttons.

Figure 8. Gateway using Dynamic IP

This connection type is the default setting of this router. Leave this setting on the column according to the following conditions:

1. You want to employ NAT. NAT allows you to use single IP address as the external one to share internet access from all of your PCs, as well as protect them from outside intruders.
2. Your ISP uses LLC Encapsulation and uses DHCP to assign an IP address when you connect to your ISP. LLC encapsulation allows multiplexing of multiple protocols over a single ATM virtual connection (VC). You can find more information on RFC 2684.

3-1-4 Gateway using Static IP

WAN  
Connection

Gateway using Static IP

(MAC: 00:c0:02:ee:45:e3)

WAN IP address:

Subnet Mask:

Gateway Address:

DNS Server 1:  (Required)

DNS Server 2:  (Optional)

DNS Server 3:  (Optional)

Save

Cancel

Help

Figure 9. Gateway using Static IP

Choose this setting according to the following conditions:

1. You want to employ NAT. NAT allows you to use single IP address as the external one to share internet access for all of your PCs, as well as protect them from outside intruders.

2. Your ISP uses LLC Encapsulation and provides you with one or more IP addresses when you apply for the service. You can find more information on RFC 2684.
- **WAN IP Address:** Enter one IP address provided by your ISP.
  - **Subnet Mask:** Enter the subnet mask values provided by your ISP.
  - **Gateway IP Address:** Your ISP will provide you with the Default Gateway IP Address.
  - **Domain Name Server (DNS):** Your ISP will provide you with at least one DNS IP Address. Multiple DNS IP settings are common. The first available DNS entry is used in most cases.

3-1-5 Gateway using Classical IP (IP over ATM)

WAN  
Connection

Gateway using Classical IP (IP over ATM)

(MAC: 00:c0:02:ee:45:e3)

WAN IP address:

Subnet Mask:

Gateway Address:

DNS Server 1:  (Required)

DNS Server 2:  (Optional)

DNS Server 3:  (Optional)

Save

Cancel

Help

Figure 10. Gateway using Classical IP

Choose this setting according to the following conditions:

1. You want to employ NAT. NAT allows you to use a single IP address as the external one to share internet access for all of your PCs, as well as protect them from outside intruders.

2. Your ISP uses **Classical IP** connection type (use LLC encapsulation and routing protocol) and provides you with one or more IP addresses when you apply for the service. You can find more information on RFC 2684.
- **WAN IP Address:** Enter the IP address provided by your ISP.
  - **Subnet Mask:** Enter the subnet mask values provided by your ISP.
  - **Gateway IP Address:** Your ISP will provide you with the Default Gateway IP Address.
  - **Domain Name Server (DNS):** Your ISP will provide you with at least one DNS IP Address. Multiple DNS IP settings are common. The first available DNS entry is used in most cases.

3-1-6 Modem using LLC Encaps



Figure 11. Modem Only

Choose this setting according to the following conditions:

- 1. You want this device acting as an ADSL modem.
- 2. Your ISP uses LLC encapsulation.

Your ISP may use DHCP to provide an IP address or to provide you with one or more IP addresses, as well as asking you to use PPPoA or PPPoE connection modes when you apply for the service. However, as you have chosen to make this device act as an modem, you have to know how to configure your PCs.

**Note:** When the router is configured in this mode, many of the routers features are disabled (firewall, filtering, etc). Therefore, the ability to configure these options from the menu on the left had side of the screen is not available.

### 3.2 Configure Wireless Security.

From the One-Page-Setup screen, select the Configure option from under the wireless section.

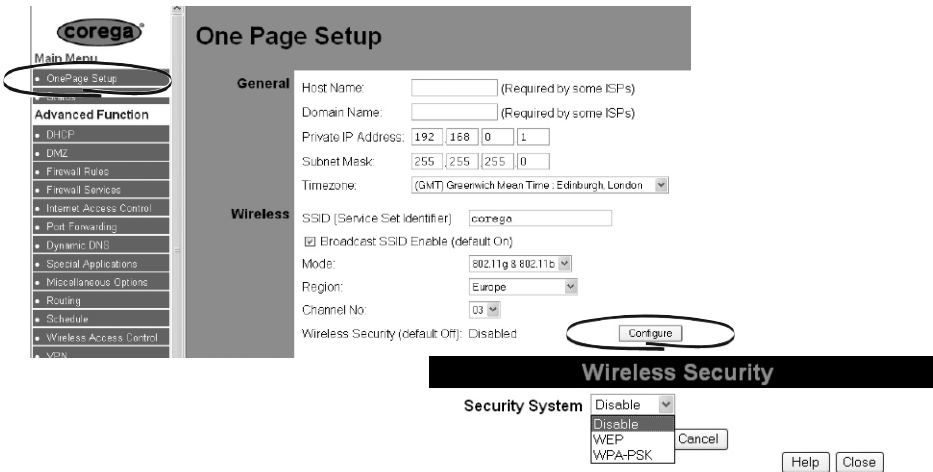


Figure 12. Configuring Wireless Security

The default wireless security setting is “disabled”. This is to ensure that all wireless devices can initially connect to the router. It is recommended that you enable wireless security on the router. Select either WEP or WPA-PSK security. All devices must use the same method of encryption.

#### 3-2-1 WEP Encryption

(Wired Equivalent Privacy), WEP is an encryption mechanism used to protect your wireless data by providing a secure communications method. WEP uses a combination of either 64 or 128-bit keys to encrypt data that is transmitted between all points in a wireless network to ensure data security. To code/decode the data transmission, all points must use the identical key.



Figure 13. WEP Encryption

- **Authentication Type:** Select either Open System or Share Key as authentication type. If you are not sure, select Auto.
- **WEP Data Encryption:** Select either “64Bit” or “128Bit” encryption algorithm from the drop-down list. There are two ways to generate WEP key:
- **Passphrase:** Enter an alphanumeric text string in this column then click the “Generate Keys” button. Four 64-bit encryption keys or one 128-bit encryption key will be created automatically.

You can enter the WEP key manually.

You may need to enter the WEP key manually to join the existing wireless network. If you are not sure which one to use, check with your network administrator.

### 3-2-2 WPA-PSK Encryption

WPA is a wireless security system with far greater protection than WEP. It avoids most of WEP's vulnerabilities. WPA has significant advantages over WEP. The encryption key used to encrypt the data is different for every packet. This TKIP (Temporal Key Integrity Protocol) mechanism shares a starting key between devices. Each device then changes their encryption key for every packet. It is extremely difficult for hackers to read messages, even if they have intercepted the data.

The image shows a 'Wireless Security' configuration window. At the top, the title 'Wireless Security' is displayed in a black bar. Below the title, the 'Security System' is set to 'WPA-PSK' via a dropdown menu. There is a text input field for 'PSK :'. The 'Encryption' is set to 'TKIP' via another dropdown menu. At the bottom, there are four buttons: 'Save', 'Cancel', 'Help', and 'Close'.

Figure 14. WEP Encryption

- **PSK** Enter the keyword key value. The data will be encrypted using a key derived from this network key. The key must be from 8 to 63 characters.
- **WPA Encryption** Select the desired option from the drop down list. (Default is TKIP).

### 3-3 Status

The Status page shows the status of the router.

#### Modem

- **Modem Status** Possible options are "Connecting" (when establishing an ADSL connection) and "Connected" (when the ADSL link is active).
- **DownStream Connection Speed** This is the speed of the ADSL link from the ISP to the router. The actual speed is dependent upon a number of parameters including your distance from the ISP's ADSL equipment, and the number of other users also connected to their equipment.
- **UpStream Connection Speed** This is the speed of the ADSL link from the router to the ISP.
- **VPI** The VPI ADSL parameter
- **VCI** The VCI ADSL parameter

#### Internet

- **Connection Method** Possible options are PPPoE, PPPoA, Dynamic IP, Static IP, Classical IP and Modem. These are selected in the One-Page-Setup.
- **Internet Connection** This shows the status, either active or idle.
- **Internet IP Address** This is the IP address assigned to the router by your ISP.

#### LAN

- **IP Address** This is the first IP address that would be assigned by the internal DHCP Server. To change this value go to DHCP.
- **Network Mask** This is the subnet mask associated with the DHCP network IP address.
- **DHCP Server** Shows either enabled or disabled.
- **MAC Address** This is the physical MAC level address of the WAN (ADSL) port of the router.

#### Wireless

- **Name (SSID)** This is the SSID of the router. The default is "corega".
- **Region** This is selected from the One-Page-Setup. Different regions support different numbers of wireless channels.
- **Channel** The active wireless channel. To change, go to One-Page-Setup.
- **Wireless AP** This shows that the internal wireless access point is active.
- **Broadcast SSID** This shows if the router is broadcasting the SSID name that it is using.

#### System

- **Device Name** Shows the device Name
- **Firmware Version** The revision of the router firmware.



## Chapter 4.0 Advanced Configuration

Most users will not need to change any advanced configuration on this router. This section is intended for users who are familiar with both wireless and routers.

### 4-1 DHCP Configuration

A DHCP (Dynamic Host Configuration Protocol) Server can automatically assign IP Addresses to each computer in your network. Unless you already have one in your LAN, it is highly recommended that you set your router to act as a DHCP server.

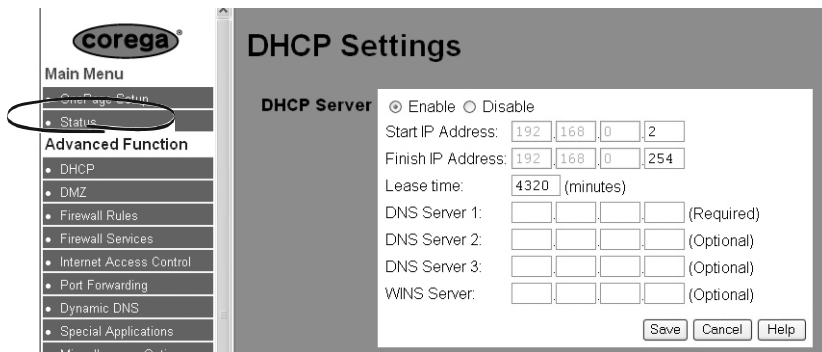


Figure 15. DHCP Settings

- **DHCP Server:** Select "Enable" to use the DHCP server internal to the router. If you already have a DHCP server in your network, set the router's DHCP option to "Disable".
- **Starting IP Address:** Enter a numerical value, from 2 to 254, for the DHCP server to start at when assigning IP Addresses.
- **Finish IP Address:** Enter a numerical value, from 2 to 254, for the DHCP server to finish at when assigning IP Addresses.
- **Lease Time:** Enter the amount of time that DHCP clients (the PCs on LAN side) can use the IP Addresses assigned by the router's DHCP server. Before the time is up, DHCP clients have to request to renew the DHCP information.
- **DNS Server:** The IP Address of the Domain Name Server, which is currently used. Multiple DNS IP settings are common. The first DNS entry will be used in most cases.
- **WINS Server:** Windows Internet Name Service (WINS Server) dynamically maps IP addresses to computer names (NetBIOS names). This allows users to access resources by computer name instead of IP addresses. If you have a WINS server on the network, enter the IP address of the server in this box.

Click the "Save" button after making any changes, or click the "Cancel" button to exit the screen without saving any changes.

4-2 DMZ

In computer networks, a DMZ (Demilitarized Zone) is a computer host or small network inserted as a “neutral zone” between a company’s private network and the outside public network. It prevents outside users from getting direct access to computers on the local LAN.

The firewall protects computers on the local LAN from unauthorised access from computers on the ADSL WAN port or the Internet. However, some applications (such as games) require a less secure network for them to interoperate. The DMZ settings allows a computer to be placed in this DMZ zone.

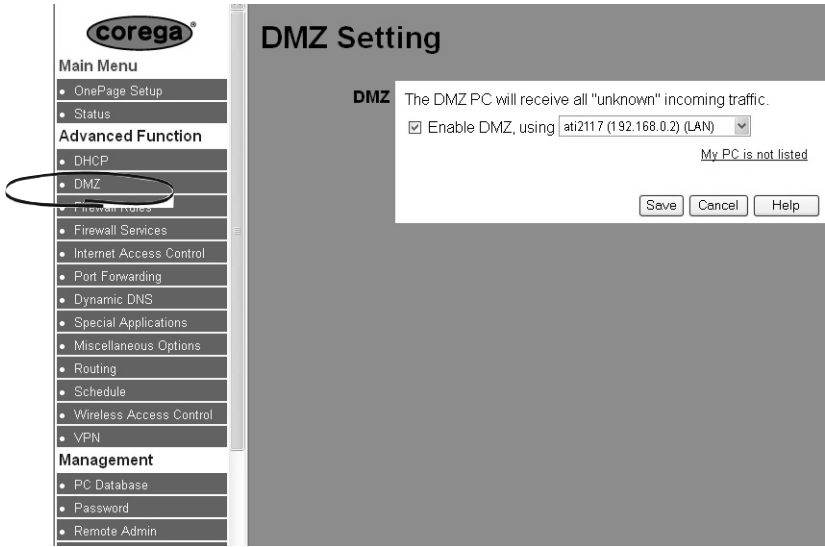


Figure 16. DMZ Settings

If you wish to enable DMZ, please check the “DMZ Enable” box and select the local computer from the drop down menu.

### 4-3 Firewall Rules

This allows users to configure the Stateful Packet Inspection Firewall to protect the user from external hackers. The firewall is enabled as default to provide the user with the maximum protection. Most users should not have to make any changes to the firewall

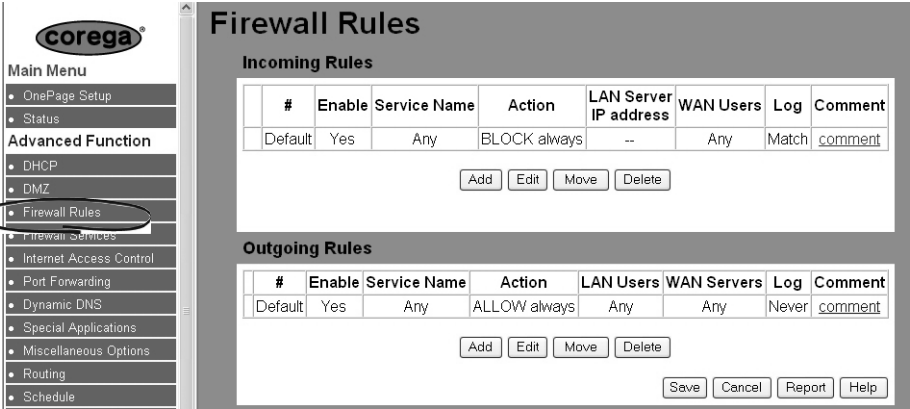


Figure 17. Firewall Rules

The default settings of the firewall are as follows:

|               |               |  |
|---------------|---------------|--|
| Incoming Data | Always Block  | This stops any unauthorised access to the router |
| Outgoing Data | Always Allows | This provides unrestricted access for users.     |

To change the Firewall, new rules can be created for both incoming and outgoing data flows. Use the **Add**, **Edit**, **Move** and **Delete** buttons to add new rules. Rules with a higher number are processed before rules with a lower number. The default rule is always the last to be processed.

- **Service** Select from the drop down list the type of application to be covered by this rule. If a service is not listed, it can be created using Firewall Services in section 4-4.
- **Action** Choose from the drop down menu of
  - BLOCK always**
  - BLOCK by schedule** - this allows the firewall to be enabled/disabled at particular times of the day.
  - ALLOW always**
  - ALLOW by schedule** - this allows the firewall to be enabled/disabled at particular times of the day.
- **LAN Users** Select which users on the LAN or wireless LAN will be effected by these rules.
- **WAN Users** Select which internet locations are effected by these rules.
- **Log** If selected, this allows the user to monitor the effectiveness of the firewall rules. Options are
  - Always** - this logs all traffic, whether it meets the requirement of the rule or not. This is useful when debugging rules.
  - Never** - select this if you do not want to monitor traffic.
  - Match** - select this if you want to log instances when the rule matches.
  - Not Match** - select this if you want to log instances when the rule does NOT match.
- **Comment** Add a user defined comment to a firewall rule so that you can remember why you set up the rule.

#### 4-4 Firewall Services

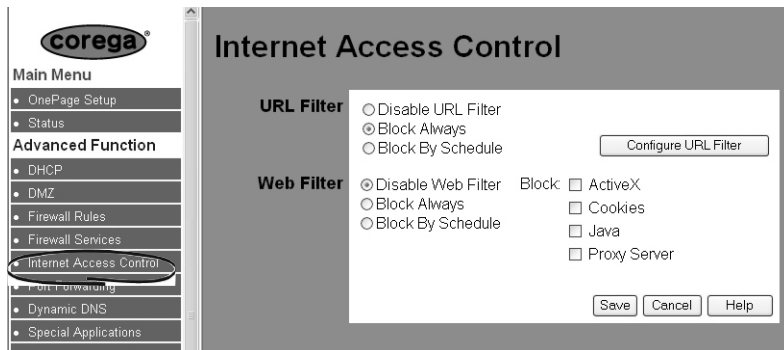
This section allows advanced users to create user defined services for use with the firewall. The following services are programmed as standard.

| Service    | TCP/UDP | Ports |
|------------|---------|-------|
| FTP        | TCP     | 20:21 |
| H.323      | TCP     | 1720  |
| HTTP       | TCP     | 80    |
| HTTPS      | TCP     | 443   |
| IDENT      | TCP     | 113   |
| IRC        | TCP/UDP | 6667  |
| NEWS       | TCP     | 144   |
| NFS        | UDP     | 2049  |
| NNTP       | TCP     | 119   |
| RCMD       | TCP     | 512   |
| REAL-AUDIO | TCP     | 7070  |
| REXEC      | TCP     | 514   |
| RTELNET    | TCP     | 107   |
| RTSP       | TCP/UDP | 554   |
| SFTP       | TCP     | 115   |
| SMTP       | TCP     | 25    |
| SNMP       | TCP/UDP | 161   |
| SNMP-TRAP  | TCP/UDP | 162   |
| SQL-NET    | TCP     | 1521  |
| SSH        | TCP/UDP | 22    |
| STRMWORKS  | UDP     | 1558  |
| TACACS     | UDP     | 49    |
| TELNET     | TCP     | 23    |
| TFTP       | UDP     | 69    |
| VDOLIVE    | TCP     | 7000  |
| VPN-IPSEC  | UDP     | 500   |
| VPN-L2TP   | UDP     | 1701  |
| VPN-PPTP   | TCP     | 1723  |

To enter a new service, use the **Add**, **Edit** and **Delete** buttons.

## 4-5 Internet Access Control

Internet Access Control allows the network administrator the ability to allow computers on the local or wireless LANs access (or denial) to specify websites or server types.



**Figure 18. Internet Access Control Main Settings**

**URL Filter:** Select from one of the three options.

- **Disable URL Filter:** In this mode, the router performs no filtering.
- **Block Always:** In this mode, the URL filters set will be active continually. See section 4-5-1 for details on setting the filters.
- **Block by Schedule:** In this mode, the URL filter will be active during the times specified by the time schedule - see section 4-11.

**Web Filter:** Select from one of the three options.

- **Disable Web Filter:** In this mode, the router performs no filtering.
- **Block Always:** In this mode, the web filters set will be active continually.
- **Block by Schedule:** In this mode, the web filter will be active during the times specified by the time schedule - see section 4-11.

Select the boxes for the web parameters that you want to block.

- Active X
- Cookies
- Java
- Proxy Server

4-5-1 Internet Access Control - URL Filter Setting

From the Internet Access Control screen, select the **Configure URL Filter** option.

URL Filter

When enabled, a request is blocked if any of these entries occur in the requested URL.

Current Filter Strings

DeleteDelete All

Add Filter String: Add

Filter Strings should be as specific as possible.

Trusted PC

☐ Allow this PC to Visit Blocked Sites

Trusted PC: Select a PC

SaveCancel

HelpClose

Figure 19. Internet Access Control - URL Filter

To add a word string to be checked when filtering, enter the characters in the **Add Filter String** and then press **Add**. All current filters will be shown in the Current Filter Strings box.

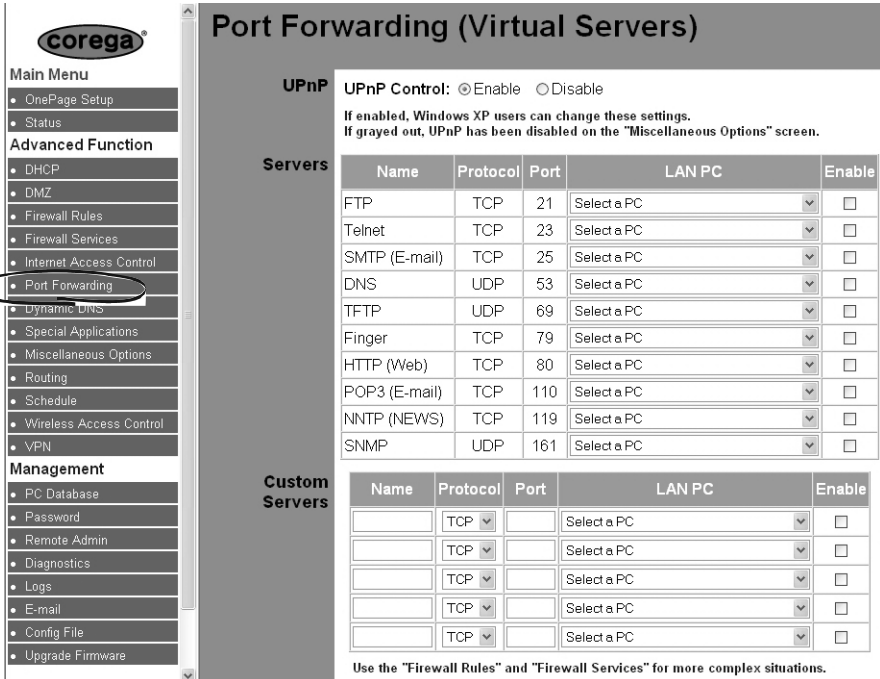
- **Delete:** Highlight a filter string in the Current Filter Strings box, then press Delete to remove the filter.
- **Delete All:** Press to remove all current filters.

Even when URL filters are set, it is still possible to allow one computer access to the blocked sites. To do this, select the **Allow this PC to Visit Blocked Sites**, and then select the **Trusted** computer from the drop-down menu of available computers.

## 4-6 Port Forwarding (Virtual Server) Settings

The Virtual Server Settings application allows up to a maximum of ten pre-defined public services and up to five user-defined services that can be accessed by external users over the internet. Service can be applications such as a Web, Email, FTP etc. Each service is provided by a dedicated network computer (server) configured with a fixed IP Address. Although the internal service addresses are not directly accessible to the external user, the router is capable of identifying the service requested by the service port number. With this information the router redirects the request to the appropriate internal IP Address. To use this application, it is recommended you use a fixed Public IP Address from your ISP. Note that the router supports only one server of any particular type.

This router also supports UPnP Forwarding. You can use either Virtual Server Settings or UPnP Forwarding by clicking the button to change setting page. Do not set the same function server to different IP Address in different setting pages.



**corega®**

**Main Menu**

- OnePage Setup
- Status
- Advanced Function**
  - DHCP
  - DMZ
  - Firewall Rules
  - Firewall Services
  - Internet Access Control
  - **Port Forwarding**
  - Dynamic DNS
  - Special Applications
  - Miscellaneous Options
  - Routing
  - Schedule
  - Wireless Access Control
  - VPN
- Management**
  - PC Database
  - Password
  - Remote Admin
  - Diagnostics
  - Logs
  - E-mail
  - Config File
  - Upgrade Firmware

## Port Forwarding (Virtual Servers)

**UPnP** UPnP Control: ☒ Enable ☐ Disable

If enabled, Windows XP users can change these settings.  
If grayed out, UPnP has been disabled on the "Miscellaneous Options" screen.

**Servers**

| Name          | Protocol | Port | LAN PC      | Enable                   |
|---------------|----------|------|-------------|--------------------------|
| FTP           | TCP      | 21   | Select a PC | <input type="checkbox"/> |
| Telnet        | TCP      | 23   | Select a PC | <input type="checkbox"/> |
| SMTP (E-mail) | TCP      | 25   | Select a PC | <input type="checkbox"/> |
| DNS           | UDP      | 53   | Select a PC | <input type="checkbox"/> |
| TFTP          | UDP      | 69   | Select a PC | <input type="checkbox"/> |
| Finger        | TCP      | 79   | Select a PC | <input type="checkbox"/> |
| HTTP (Web)    | TCP      | 80   | Select a PC | <input type="checkbox"/> |
| POP3 (E-mail) | TCP      | 110  | Select a PC | <input type="checkbox"/> |
| NNTP (NEWS)   | TCP      | 119  | Select a PC | <input type="checkbox"/> |
| SNMP          | UDP      | 161  | Select a PC | <input type="checkbox"/> |

**Custom Servers**

| Name | Protocol | Port | LAN PC      | Enable                   |
|------|----------|------|-------------|--------------------------|
|      | TCP      |      | Select a PC | <input type="checkbox"/> |
|      | TCP      |      | Select a PC | <input type="checkbox"/> |
|      | TCP      |      | Select a PC | <input type="checkbox"/> |
|      | TCP      |      | Select a PC | <input type="checkbox"/> |
|      | TCP      |      | Select a PC | <input type="checkbox"/> |

Use the "Firewall Rules" and "Firewall Services" for more complex situations.

Figure 20. Virtual Server Settings

**UPnP** UPnP (Universal Plug and Play) is a standard introduced from Microsoft and UPnP Forum for interoperability. Currently, this function supported by this device allows you to set a virtual server from a Windows OS that supports UPnP, such as Windows XP.

- **UPnP Control:** If enabled, the Windows XP OS will automatically communicate with the router to set up ports to allow applications such as Messenger to operate without the user having to manually configure ports. If this section is 'grey' and cannot be accessed, then enable the UPnP option in section 4-9.

**Servers** The pre-determined Server type have been setup, these are: FTP, Telnet, SMTP (Email), DNS, TFTP, Finger, HTTP (Web), POP-3 (Email), NNTP (News) & SNMP. Set up individual network computers on the LAN to act as servers and configure each with a **fixed IP Address**.

- **Select a PC:** From the drop-down menu, select the PC that will be providing the Virtual Server function.
- **Enable:** With a PC selected, the port forwarding will only become active if there is a tick in the enable box.

**Custom Server** Set up individual network computers on the LAN to act as servers and configure each with a **fixed IP Address**.

- **Name:** Give the service that you are setting up an arbitrary name.
- **Protocol:** You can specify the protocol type as "TCP" or "UDP" from the drop-down list. If you are not sure which one to select, choose "Both".
- **Ports:** Enter the desired service port numbers in the "Ports" fields.
- **Select a PC:** From the drop-down menu, select the PC that will be providing the Virtual Server function.
- **Enable:** With a PC selected, the port forwarding will only become active if there is a tick in the enable box.

4-7 Dynamic DNS (DDNS)

“DDNS” is an acronym for Dynamic Domain Name Service. Whenever you set up the web servers, mail servers, or sometimes ftp servers, you need “Domain Name” to help internet users reach your servers easily.

The internet actually runs on IP Addresses which are in numerical order, for example “66.37.215.53”. These IP Addresses identify the location of each device connected to the internet. However, the human brain does not easily remember this numbering system, so a system that allocates domain name such as “www.dyndns.org” provides an easier method. If you type “66.37.215.53” or “www.dyndns.org” in the web browser’s address bar, the browser will show the same web page. This is because both methods relate to the same web server. The “Domain Name Servers” used to manage the internet will translate “www.dyndns.org” into the IP Address “66.37.215.53” in order to allow your browser to find the web server and display the correct web page in your browser. If your “WAN Connection Type”, as shown in One Page Setup section, is “Obtain IP Address Automatically”, “PPPoE”, or “PPTP” with dynamic IP address assigned by ISP, it will cause an error when you set up the public computer servers in your LAN side PCs. Internet users may not be able to reach your servers because your WAN side IP address may change each time you initiate the connection to your ISP. The DDNS function will help to map your IP address to your domain name when your ISP assigns a new dynamic IP Address. Note that this DDNS function acts as the client appliance of DDNS service and is only able to be used in conjunction with the service provided by DynDNS.org. Before you begin using this function, you will need to apply to DynDNS.org to be able to use the service. Please visit [www.dyndns.org](http://www.dyndns.org) for further information.

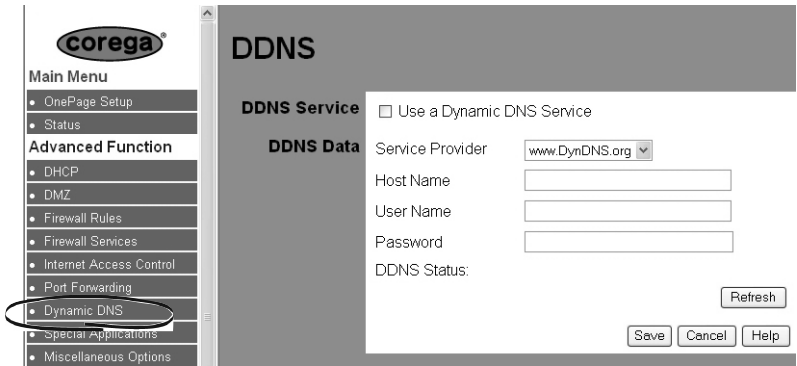


Figure 21. DDNS Settings

- **DDNS Service:** Check the “Enable” option if you wish to activate this function.
  - **Service Provider:** This is the URL of the company that will provide the DDNS Service. Presently, this is set for [www.DynDNS.org](http://www.DynDNS.org)
  - **Host Name:** DynDNS.org, will provide you with a Host Name. Enter this name in the “Host Name” field.
  - **Username:** After you have applied for the DDNS service from DynDNS.org, you will be issued with a Username. Enter this username in the “Username” field.
  - **Password:** DynDNS.org, will also issue you with a password. Enter the detail in the “Password” field.
- Click the “Save” button after making any changes, or click the “Cancel” button to exit the screen without saving any changes.



## 4-8 Special Applications

This feature is for Internet applications which normally cannot work through the built-in firewall. If an Internet application does not work, you can try defining it here. You will need detailed information about the application from the provider of the service or application. Note that the terms "Incoming" and "Outgoing" refer to traffic from the client (PC) viewpoint.

| Enable                       | Name | Outgoing Ports |       |        | Incoming Ports |       |        |
|------------------------------|------|----------------|-------|--------|----------------|-------|--------|
|                              |      | Type           | Start | Finish | Type           | Start | Finish |
| 1. <input type="checkbox"/>  |      | TCP            |       |        | TCP            |       |        |
| 2. <input type="checkbox"/>  |      | TCP            |       |        | TCP            |       |        |
| 3. <input type="checkbox"/>  |      | TCP            |       |        | TCP            |       |        |
| 4. <input type="checkbox"/>  |      | TCP            |       |        | TCP            |       |        |
| 5. <input type="checkbox"/>  |      | TCP            |       |        | TCP            |       |        |
| 6. <input type="checkbox"/>  |      | TCP            |       |        | TCP            |       |        |
| 7. <input type="checkbox"/>  |      | TCP            |       |        | TCP            |       |        |
| 8. <input type="checkbox"/>  |      | TCP            |       |        | TCP            |       |        |
| 9. <input type="checkbox"/>  |      | TCP            |       |        | TCP            |       |        |
| 10. <input type="checkbox"/> |      | TCP            |       |        | TCP            |       |        |
| 11. <input type="checkbox"/> |      | TCP            |       |        | TCP            |       |        |
| 12. <input type="checkbox"/> |      | TCP            |       |        | TCP            |       |        |

Save Cancel Help

Figure 22. Special Applications

Operation is as follows:

1. When outgoing traffic from a PC uses an outgoing port defined as a Special Application, the Router records the PC and Special Application.
2. When an incoming connection is received which uses an incoming port for that Special Application, that traffic is forwarded to the PC. (Without the Special Application entry, the incoming traffic would be discarded.)

**Note:** Only 1 PC can use a Special Application at any time. After each use, there will be a "time-out" period before the next PC can use the same Special Application.

Each Special Application must use unique port numbers. You can not enable two Special Applications which use the same port number.

The Special Applications feature is triggered by Outgoing traffic. So it will not help with incoming connections. (The Virtual Server and DMZ features can be used to determine the destination for incoming connections.)

- **Name** Enter a descriptive name to identify this Special Application. Use the checkbox to Enable or Disable the Special Application as required.

### Incoming & Outgoing Ports

- **Type** Select the protocol (TCP or UDP) used when you receive (incoming) or send (outgoing) data from the special application or service. (Note: Some applications use different protocols for outgoing and incoming data).
- **Start** Enter the beginning of the range of port numbers used by the application server, for data you receive (incoming) or send (outgoing). If the application uses a single port number, enter it in both the "Start" and "Finish" fields.
- **Finish** Enter the end of the range of port numbers used by the application server, for data you receive (incoming) or send (outgoing).

4-9 Miscellaneous Options

This section allows users to configure some Miscellaneous options in the router.

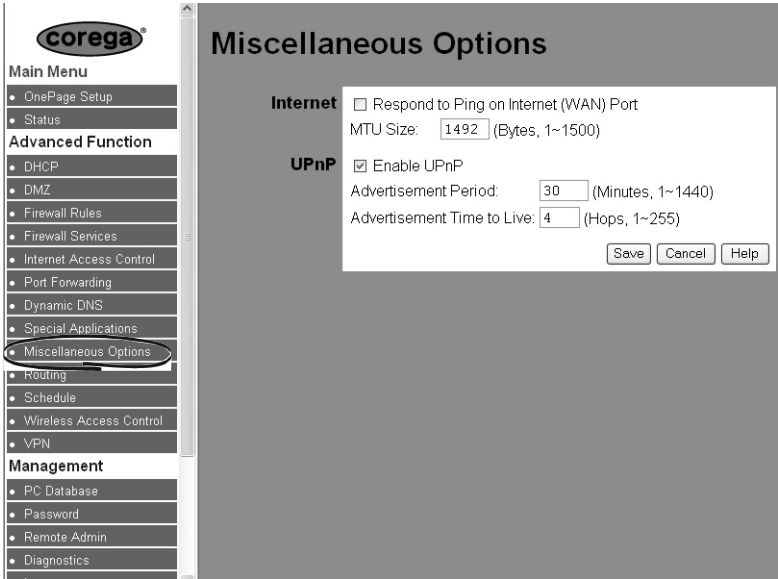


Figure 23. Miscellaneous Options

Internet

- **Respond to Ping:** If this option is **enabled**, then the router will respond to a ping request on the LAN port. This option is sometimes useful when you want to test connections across the Internet. When **disabled**, the router will not respond, making the network more secure.
- **MTU Size:** This is the Maximum Transmission Unit size. This is the maximum amount of data that can be transmitted over the ADSL link as a single packet. The value can be set between 1 and 1500. Changing this value may be advised by your ISP.

UPnP

- **Enable UPnP:** When enabled, it allows computers compatible with the UPnP (Universal Plug and Play) specification to automatically discover and configure the router. (Normally, this means Windows XP). If disabled, the router will not respond to UPnP requests.
- **Advertisement Period:** This is the value in minutes (range 1-1400) that the router will. This is the length of time that the router will advertise that it supports UPnP after power up or reset.
- **Advertisement Time to Live:** This value determines the number of routers that the UPnP packets will transverse before they are deleted from the network.

## 4-10 Routing

The Routing feature allows the router to exchange routing information with other routers in the network.

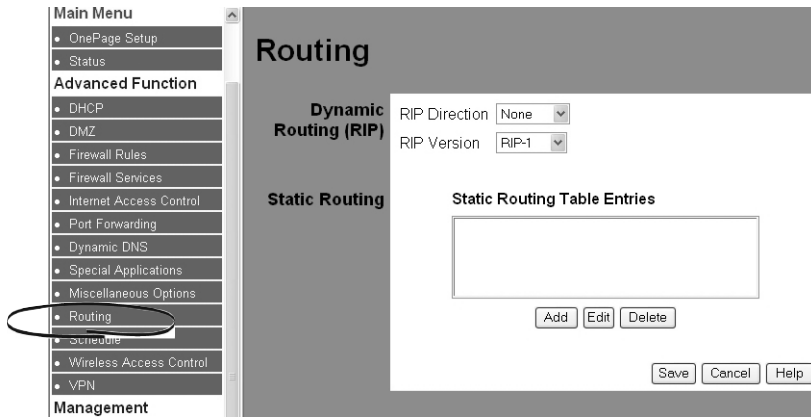


Figure 24. Routing

### Dynamic Routing (RIP)

- **RIP Direction** From the drop-down list, select one of the routing types:
  - "None"
  - "In Only"
  - "Out Only"
  - "Both"
- **RIP Version** From the drop-down list, select one of the routing types:
  - Disabled
  - "RIP-1"
  - "RIP-2B"
  - "RIP-2M"

Click the "Save" button after making any changes, or click the "Cancel" button to exit the screen without saving any changes.

4-11 Time Schedule

This feature allows you to limit connection availability according to a nominated time of day schedule. Up to two active sessions are allow on each day of the week.

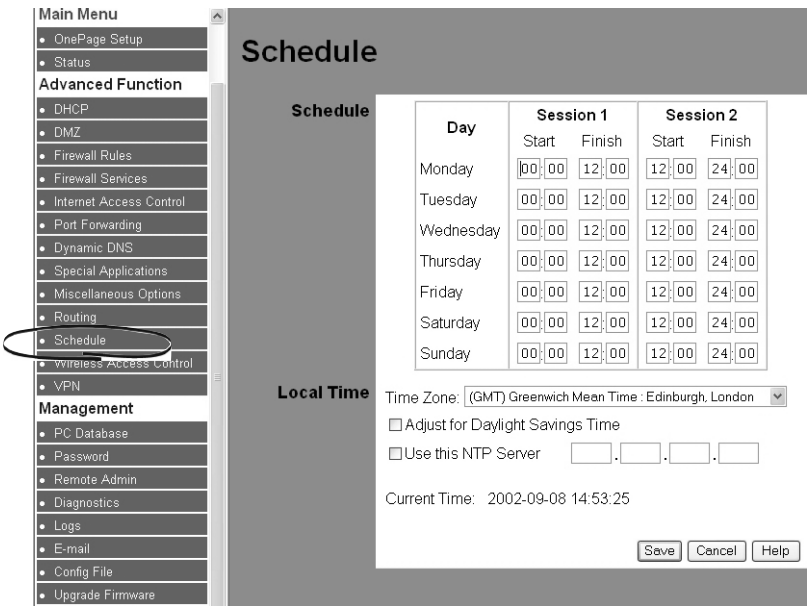


Figure 25. Time Schedule

Schedule

- **Sessions:** For each day of the week, the user can define up to two time periods when the schedule will be active. The schedule is used in conjunction with Internet Access Control as described in section 4-5.

For example, to block access to specific websites during working hours, then set the schedule as follows:

| Day       | Session 1 | Session 2 |   |
|-----------|-----------|-----------|---|
| Monday    | 0900-1200 | 1300-1800 |   |
| Tuesday   | 0900-1200 | 1300-1800 |   |
| Wednesday | 0900-1200 | 1300-1800 |   |
| Thursday  | 0900-1200 | 1300-1800 |   |
| Friday    | 0900-1200 | 1300-1800 |   |
| Saturday  | 0000-0000 | 0000-0000 | Left blank to allow access all the time |
| Sunday    | 0000-0000 | 0000-0000 | Left blank to allow access all the time |

Local Time

- **Time Zone:** Select from the drop-down menu the time zone for the router. This is needed to set the clock for the schedule.
- **Adjust for Daylight Savings Time:** During summer months, with this option selected, the schedule will operate one hour earlier.
- **NTH Server:** Enter the address of a Network Time Protocol Server, which will be used to provide the correct time to the router. (This is sometimes referred to as SNIP - Simple Network Time Protocol). For further information, see [www.NTH.org](http://www.NTH.org).

Click the "Save" button after making any changes, or click the "Cancel" button to exit the screen without saving any changes.

## 4-12 Wireless Access Control

Wireless Access Control provides an additional level of security allowing the network administrator to block unauthorised **wireless** clients from connecting to the router.

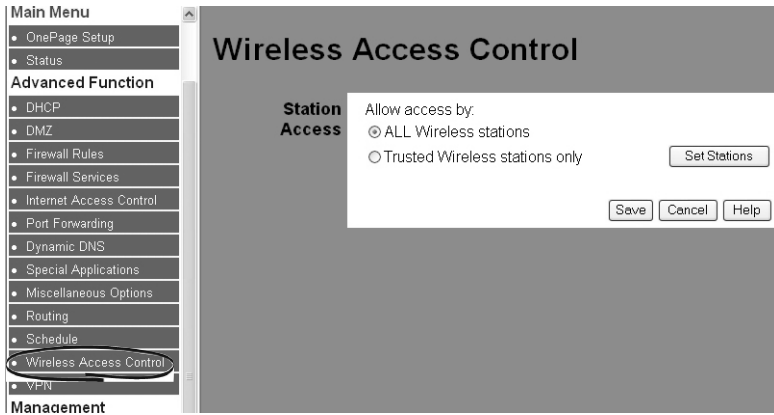


Figure 26. Wireless Access Control

### Station Access

- **ALL Wireless Stations:** If this is selected, then all wireless clients can connect to the router without any additional security.
- **Trusted Wireless stations only:** If this is selected, then only wireless clients that have been authorised can connect to the router. To give wireless clients authorisation, select **Set Stations**.
- **Set Stations:**

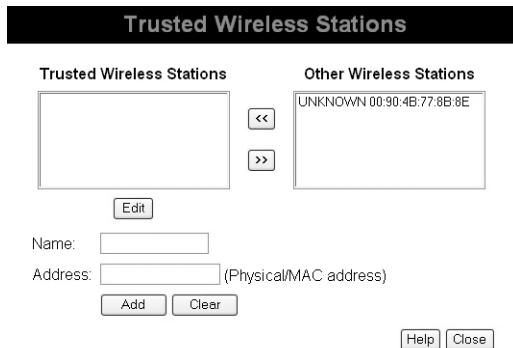


Figure 27. Wireless Access Control - Trusted Wireless Stations

To enter a "trusted station" or "other station", perform the following:

- **Name** Enter the name of the station
- **Address** Enter the MAC address of the station

Select **Add** to enter the station.

Stations can be moved between "trusted" and "other" by highlighting the station and using the arrow buttons.

4-13 Virtual Private Network (VPN) Settings

A Virtual Private Network (VPN) allows users to use the internet to make the equivalent of a direct connection (private network) between two offices. Private networks should be extremely secure, therefore when using the internet to make a VPN, data encryption must be used to ensure a high level of data security.

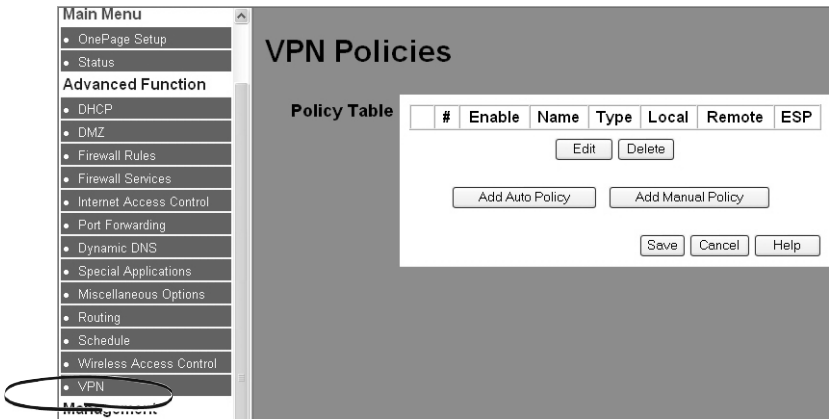


Figure 28. VPN Policies

The table shows all the current VPN Policies enabled on the router. If there are multiple policies, and traffic is covered by two or more policies, then the first matching policy will be used.

- **Enable:** Use this checkbox to enable or disable a policy. This allows policies to be disabled without having to delete the policy.
- **Name:** Each policy has a unique name.
- **Type:** Policies can be created as either Manual or Auto. If a VPN is created as a Manual policy, then all settings including keys will need to be entered manually at both ends of the VPN link. If a VPN is created as an Auto policy, then some settings will be generated automatically. Use of the Auto mode requires the use of IKE (Internet Key Exchange) protocol to perform negotiations between the two VPN end points.
- **Local:** This is the IP address, or range of IP addresses for the local LAN.
- **Remote:** This is the IP address, or range of IP addresses for the remote LAN.
- **ESP:** This is the Encapsulating Security Payload. This specifies the encryption protocol used for the VPN data.

VPN - Manual Policy

General

Policy Name

Remote VPN Endpoint

Address Type: Fixed IP Address

Address Data:

☒ NETBIOS Enable

Local LAN

IP Address

Subnet address

Single/Start IP address:

192

168

0

1

Subnet Mask

255

255

255

0

Remote LAN

IP Address

Single PC - no subnet

Single/Start IP address:

Subnet Mask

ESP Configuration

SPI - Incoming☐ (Hex, 3 Characters)

SPI - Outgoing☐ (Hex, 3 Characters)

Encryption

3DES

Key:

(DES - 8 chars; 3DES - 24 chars)

Authentication

SHA-1

Key:

(MD5 - 16 chars; SHA-1 - 20 chars)

Back

Save

Cancel

Help

Figure 29. Adding a Manual VPN

General

- **Policy Name:** The router allows the user to set up multiple VPN configurations. Each configuration has a unique name.  
**Note!** The Policy Name set here does not always have to match the name used at the other end of the Tunnel. However, certain VPN applications require a Tunnel to have the same name at both ends of the Tunnel. If the other end point with which you want to establish the Tunnel does not use this router, it is important that you give the other side precise set up instructions and ensure that these are followed.
- **Remote VPN Endpoint:** The remote end of the VPN can be defied as either a fixed IP address, or as a Fully Qualified Domain Name.

| Address Type                | Address Data   | Comments   |
|-----------------------------|----------------|--|
| Fixed IP Address            | 123.123.1.1    | Enter the value of the remote device's Fixed IP address of the WAN port.                             |
| Fully Qualified Domain Name | www.remote.com | The URL of the remote end point. Note, DDNS must be enabled to resolve this name into an IP address. |
- **NETBIOS Enable:** Enable this checkbox if you wish Microsoft's NETBIOS networking protocol to be transported over the VPN tunnel.

Local LAN

- **IP Address:** This allows the local LAN VPN to be directed to either
  - Single IP Address
    - **IP Address** Enter the IP address of the single device on the local LAN that can access the VPN.
    - **Subnet Mask** Not Applicable
  - Subnet Address
    - **IP Address** Enter the IP address of the local LAN that can access the VPN.
    - **Subnet Mask** Enter the subnet of local LAN that can access the VPN.

Remote LAN

- **IP Address:** This allows the Remote LAN VPN to be directed to either
  - Single PC      Use this when the remote device is a single PC using Dynamic IP and with no LAN.
    - **IP Address**      Leave blank.
    - **Subnet Mask**      Leave blank.
  - IP Address
    - **IPAddress**      Enter the IP address of the single device on the Remote LAN that can access the VPN.
    - **Subnet Mask**      Not Applicable
  - Subnet Address
    - **IP Address**      Enter the IP address of the Remote LAN that can access the VPN.
    - **Subnet Mask**      Enter the subnet of the Remote LAN that can access the VPN.

ESP Configuration

- **SPIN - Incoming:** The value set here must match the SPIN - Outgoing value at the other end of the VPN Tunnel. Conversely, the “**SPIN - Outgoing**” must match the SPIN - Incoming value at the other end. Only numeric characters can be used in both these fields.
- **SPIN - Outgoing:** The value set here must match the SPIN - Incoming value at the other end of the VPN Tunnel. Conversely, the “**SPIN - Incoming**” must match the SPIN - Outgoing value at the other end. Only numeric characters can be used in both these fields.
- **Encryption:** Select either DES or 3DES from the drop down list. 3DES is default as it is the more secure option. Both ends of the Tunnel must use the **same encryption type**.
- **Encryption Key:** Because this is a Manual Policy, the user must enter the DES or 3DES encryption key.
- **Authentication:** This item adds another level of security. There are two types of authentication: “**MD5**” and “**SHA**”. Both ends of the Tunnel must use the same **authentication type**.
- **Authentication Key:** Because this is a Manual Policy, the user must enter the MD5 or SHA authentication key.



### 4-13-2 Add Auto Policy

VPN - Auto Policy

General

Policy Name

Remote VPN Endpoint Address Type: Dynamic IP address

Address Data: n/a

☒ NetBIOS Enable

Local LAN

IP Address Subnet address

Single/Start IP address: 192.168.0.1

Subnet Mask: 255.255.255.0

Remote LAN

IP Address Single PC - no Subnet

Single/Start IP address:

Subnet Mask:

IKE

Direction Responder only

Exchange Mode Main Mode

Diffie-Hellman (DH) Group Auto

Local Identity Type WAN IP Address

Data n/a

Remote Identity Type IP Address

Data n/a

Parameters

Encryption Algorithm 3DES

Authentication Algorithm Auto

Pre-shared Key

SA Life Time 28800 (Seconds)

☐ Enable PFS (Perfect Forward Security)

Back

Save

Cancel

Help

Figure 30. Adding an Auto VPN

#### General

- Policy Name:** The router allows the user to set up multiple VPN configurations. Each configuration has a unique name.
- Note!** The Policy Name set here does not always have to match the name used at the other end of the Tunnel. However, certain VPN applications require a Tunnel to have the same name at both ends of the Tunnel. If the other end point with which you want to establish the Tunnel does not use this router, it is important that you give the other side precise set up instructions and ensure that these are followed.
- Remote VPN Endpoint:** The remote end of the VPN can be defined as either a fixed IP address, or as a Fully Qualified Domain Name.
 

| Address Type                | Address Data   | Comments   |
|-----------------------------|----------------|--|
| Fixed IP Address            | 123.123.1.1    | Enter the value of the remote device's Fixed IP address of the WAN port.                             |
| Fully Qualified Domain Name | www.remote.com | The URL of the remote end point. Note, DDNS must be enabled to resolve this name into an IP address. |
- NETBIOS Enable:** Enable this checkbox if you wish Microsoft's NETBIOS networking protocol to be transported over the VPN tunnel.

#### Local LAN

- IP Address:** This allows the local LAN VPN to be directed to either
 

|                     |   |  |
|---------------------|---|--|
| - Single IP Address | <b>IP Address</b><br><b>Subnet Mask</b> | Enter the IP address of the single device on the local LAN that can access the VPN.<br>Not Applicable                    |
| - Subnet Address    | <b>IP Address</b><br><b>Subnet Mask</b> | Enter the IP address of the local LAN that can access the VPN.<br>Enter the subnet of local LAN that can access the VPN. |

## Remote LAN

- **IP Address:** This allows the Remote LAN VPN to be directed to either
  - Single PC      Use this when the remote device is a single PC using Dynamic IP and with no LAN.
    - **IP Address**      Leave blank.
    - **Subnet Mask**      Leave blank.
  - IP Address      • **IP Address**      Enter the IP address of the single device on the Remote LAN that can access the VPN.
  - **Subnet Mask**      Not Applicable
  - Subnet Address      • **IP Address**      Enter the IP address of the Remote LAN that can access the VPN.
  - **Subnet Mask**      Enter the subnet of the Remote LAN that can access the VPN.

## IKE

- **Direction** This setting is used when determining if the IKE policy matches the current traffic. Select the desired option.
  - Responder only - Incoming connections are allowed, but outgoing connections will be blocked.
  - Initiator and Responder - Both incoming and outgoing connections are allowed.
- **Exchange Mode** IPsec has 2 possibilities - "Main Mode" and "Aggressive Mode". Currently, only "Main Mode" is supported. Ensure the remote VPN endpoint is set to use "Main Mode".
- **Diffie-Hellman (DH) Group** The Diffie-Hellman algorithm is used when exchanging keys. The DH Group setting determines the number of bit size used in the exchange. This value must match the value used on the remote VPN Gateway.
- **Local Identity Type** Select the desired option to match the "Remote Identity Type" setting on the remote VPN endpoint.
  - WAN IP Address - your Internet IP address.
  - Fully Qualified Domain Name - your domain name.
  - Fully Qualified User Name - your name, E-mail address, or other ID.
- **Local Identity Data** Enter the data for the selection above. (If "WAN IP Address" is selected, no input is required.)
- **Remote Identity Type** Select the desired option to match the "Local Identity Type" setting on the remote VPN endpoint.
  - IP Address - The Internet IP address of the remote VPN endpoint.
  - Fully Qualified Domain Name - the Domain name of the remote VPN endpoint.
  - Fully Qualified User Name - the name, E-mail address, or other ID of the remote VPN endpoint.
- **Remote Identity Data** Enter the data for the selection above. (If "IP Address" is selected, no input is required.)

## SA Parameters

- **Encryption** Encryption Algorithm used for both IKE and IPsec. This setting must match the setting used on the remote VPN Gateway.
- **Authentication** Authentication Algorithm used for both IKE and IPsec. This setting must match the setting used on the remote VPN Gateway.
- **Pre-shared Key** The key must be entered both here and on the remote VPN Gateway. This method does not require using a CA (Certificate Authority).
- **SA Life Time** This determines the time interval before the SA (Security Association) expires. (It will automatically be re-established if necessary.) While using a short time period (or data amount) increases security, it also degrades performance. It is common to use periods over an hour (3600 seconds) for the SA Life Time. This setting applies to both IKE and IPsec SAs.
- **IPsec PFS (Perfect Forward Secrecy)** If enabled, security is enhanced by ensuring that the key is changed at regular intervals. Also, even if one key is broken, subsequent keys are no easier to break. (Each key has no relationship to the previous key.)
 

This setting applies to both IKE and IPsec SAs. When configuring the remote endpoint to match this setting, you may have to specify the "Key Group" used. For this device, the "Key Group" is the same as the "DH Group" setting in the IKE section.

## Chapter 5-0 Management

Topics dealt with in this section are to do with the management of the router.

### 5-1 PC Database

The PC Database contains a list of all the computers attached to the local LAN and wireless LAN. This database performs the following functions:

It maintains a list of all the DHCP Clients which have been allocated a Dynamic IP address by the router.

The router will allocate the same Dynamic IP address to clients when they reconnect.

This allows users to set up virtual servers without having to use static IP addresses. The router will also identify attached computers by their unique MAC address.

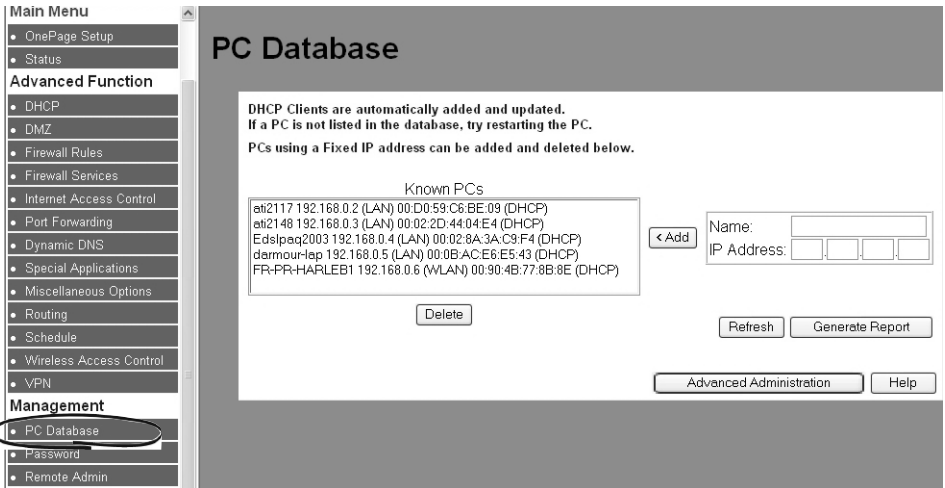


Figure 31. PC Database

- **Known PCs:** This shows the computers connected to the local LAN. They are identified by
  - Name
  - IP Address
  - MAC Address
- **Add:** This will add a new PC to the list. If the PC is not connected to the LAN, it will not be added. This is because when the Add button is pressed, the PC will be send a ping request to determine it's hardware MAC address. If no response to the ping is received, then the new entry is not made.
- **Delete:** Highlight the computer in the Known PCs list, and press Delete to remove a computer from the database. This should be performed if the PC has been removed from the LAN, and you need to free the dynamic IP address.
- **Generate Report:** This will invoke a read only list of all the computers in the PC Database.
- **Advanced Administration:** See section 5-1-1.

5-1-1 Advanced Administration

This allows the user to add computers with Fixed IP addresses to the PC Database or to add a computer to the list which are not connected to the local LAN.

PC Database - Advanced

PC database entries can be added, edited or deleted. When adding an entry for a PC which is not connected, the user must provide the MAC (hardware) address

Known PCs

eti2117 192.168.0.2 (LAN) 00:D0:59:C6:BE:09 (DHCP)  
eti2148 192.168.0.3 (LAN) 00:02:2D:44:04:E4 (DHCP)  
Edslpaq2003 192.168.0.4 (LAN) 00:02:8A:3A:C9:F4 (DHCP)  
clarmour-lap 192.168.0.5 (LAN) 00:0B:AC:E6:E5:43 (DHCP)  
FR-PR-HARLEB1 192.168.0.6 (WLAN) 00:90:4B:77:8B:8E (DHCP)

Edit

Delete

PC Properties

Name:

IP Address:

☐ Automatic (DHCP Client)

☐ DHCP Client - reserved IP address: 

1921680

☒ Fixed IP address (set on PC):

MAC Address: 

☐ Automatic discovery (PC must be available on LAN)

☒ MAC address is

Add as New Entry

Update Selected PC

Clear Form

Refresh

Generate Report

Standard Screen

Help

Figure 32. PC Database - Advanced Administration

Properties

- **Name:** Enter a name of the computer that you wish to add to the database.
- **Address:** Enter either the reserved DHCP address or the Fixed IP address that you wish this computer to use.
- **MAC Address:** If the computer is attached to the LAN, the router can auto-discover the hardware MAC address using the ping command. If the computer is not attached, manually enter the computer's MAC address
- **Add as New Entry:** Click this button to add the new computer details to the PC Database.
- **Clear Form:** Click this button to clear all the entries in the form.
- **Generate Report:** This will invoke a read only list of all the computers in the PC Database.

ENGLISH

34

## 5-2 Password

This feature allows the administrator to manage the router's password. For security reasons, it is strongly recommended that you set Passwords so that only authorized persons are able to manage this router. If the Password is left blank, all users on your network can access this router simply by entering the unit's IP Address into their web browser.

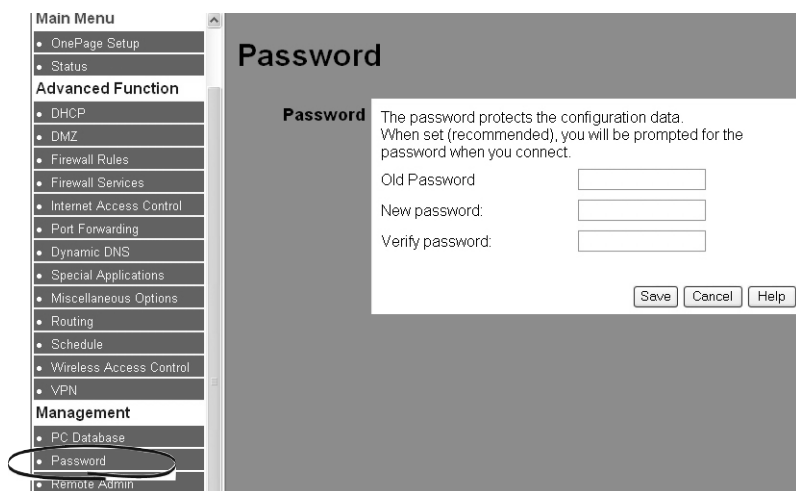


Figure 33. Password

- **Old Password:** The existing password must be entered before the password can be changed.
- **New Password:** Enter the new password for the router.
- **Verify Password:** Re-Enter the new password for the router.

5-3 Remote Administration

This feature allows the router to be managed from a device on the Internet. (i.e. via the ADSL WAN port).

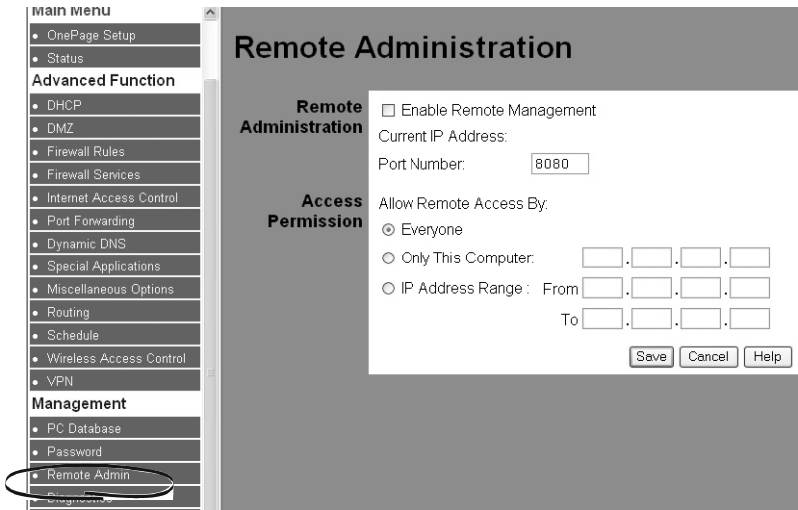


Figure 34. Remote Administration

Remote Administration

- **Enable:** Check the tickbox to allow the router to be managed via the Internet. If disabled, the router will not respond to requests via the ADSL WAN port.

This screen also shows the Current IP address of the WAN port of the router.

- **Port Number:** Enter a value between 1024 and 65535. The default value is 8080. Normal HTTP (web) connections will use port 80. However, this may be used for a virtual server, thus preventing the use of remote administration.

To access this router from the Internet, start a browser and point the browser to the the Current IP Address, followed by the Port Number as shown:

`http://ip_address:port_number` i.e. `http://145.35.54.9:8080`

You will then be prompted for the password as set in section 5.2.

Access Permission

- **Everyone:** Check this box if you want to allow any computer on the Internet to be able to manage the router (assuming they know the password).
- **Only This Computer:** Check this box if you want to allow **only one** computer on the Internet to be able to manage the router (assuming they know the password). Enter the IP address of the computer.
- **IP Address Range:** Check this box if you want to allow **a number of** computers on the Internet to be able to manage the router (assuming they know the password). Enter the start and finish IP addresses of the computers.

## 5-4 Network Diagnostics

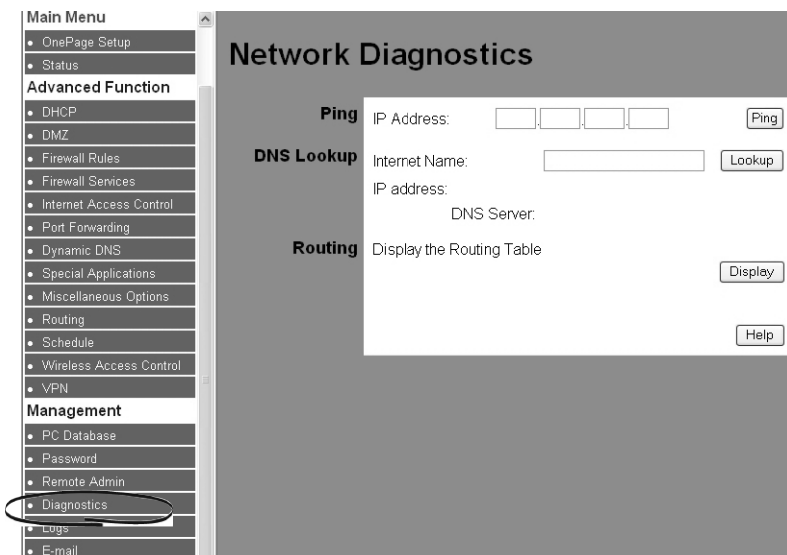


Figure 35. Network Diagnostics

**Ping** This function allows you to test the connection between the router and LAN or between the router and internet.

- **IP Address:** Enter an IP address of a device which is either on the Local LAN or on the WAN. Then click **Ping**.

**DNS Lookup** This function allows you to look up the address of a Domain Name of URL using a Domain Name Server. (Note that the DDNS must be setup for this to work - see section 4-7.)

- **Internet Name:** Enter the Domain Name or URL that you wish to look up. Then press **Lookup**.

**Routing** This function displays the internal routing table in the router.

- **Display:** Click Display to show the routing table.

## 5-5 Logs

The Log application provides the administrator with the ability to trace internet connections. When viewing the Log information, an administrator can send the record to specific LAN PCs to have real time monitoring.

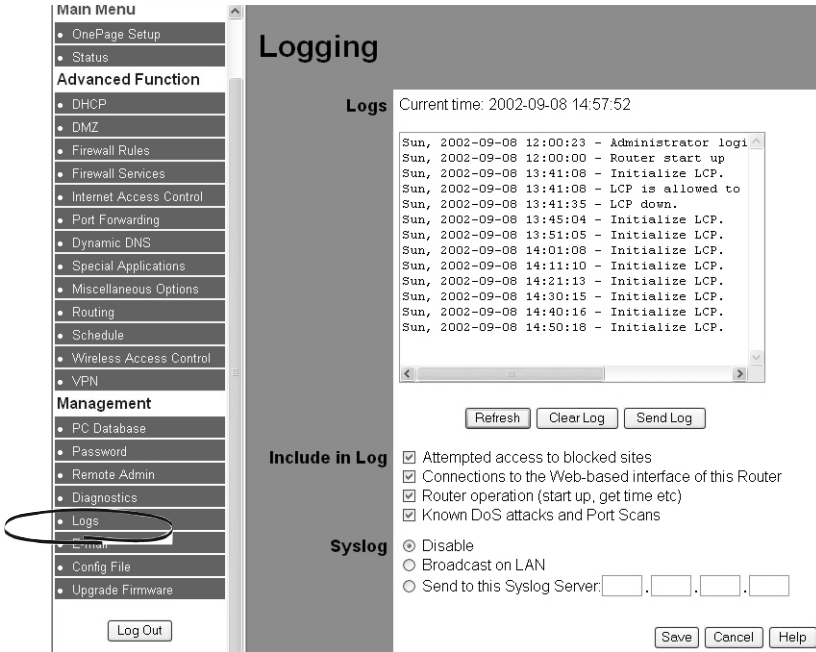


Figure 36. Log Settings

**Logs** This shows the current log file for the router.

- **Refresh:** Clicking this box refreshes the log screen to show the most recent entries.
- **Clear Log:** Clicking this box deletes all the entries in the log.
- **Send Log:** Clicking this box sends immediately the current log to an email account.

**Include in Log** Use these checkboxes to determine which events will be included in the log file.

- **Attempted Access to Blocked Sites:** This shows when attempts have been made to access sites which have been blocked. See section 4-5 Internet Access Control.
- **Connections to the Web-based interface of this Router:** This logs connections that have been made to this router via the WAN port.
- **Router Operation:** This logs internal router operations such as start up, get time etc.
- **DoS Attacks and Port Scans:** This logs potential security breaches in the form of Denial of Service and Port Scan attacks.

**Syslog:** The log files can be sent to a Syslog Server

- **Disable:** When checked, the logs are not send to the server.
- **Broadcast on LAN:** The log is broadcast on the local LAN. This is useful if the Syslog Server has a dynamic IP address.
- **Send to Syslog Server:** If the Syslog server has a fixed IP address, enter this address and the log file will be send directly to the server.



## 5-6 E-Mail

This allows the status of the router to be emailed to a specific email account.

Figure 37. E-Mail Settings

### E-mail Notification

- **Turn E-mail Notification on:** Check this box if you wish to enable email notification.
- **Send this to E-mail Address:** Enter the email address of the user that wishes to receive the notification.
- **Outgoing SMTP Mail Server:** Enter the address of the Simple Mail Transport Server mail server
- **My SMTP Mail Server requires authentication:** Check this box if your SNMP server requires authentication (username and password).
- **User Name:** Enter your SNMP Mail Server Username.
- **Password:** Enter your SNMP Mail Server Password.

### E-mail Alerts Send E-Mail alerts immediately upon the following actions.

- **DoS Attack:** If checked, an e-mail will be sent immediately whenever the router is under a Denial of Service attack.
- **Port Scan Attack:** If checked, an e-mail will be sent immediately whenever the router is under a Port Scan attack.
- **Attempt to access blocked site:** If checked, an e-mail will be sent immediately whenever the router is under a Denial of Service attack.

### E-mail Logs Send E-Mail alerts according to the following schedule

Logs can be sent, or disabled.

| Schedule         | Comment  |
|------------------|--|
| Never            | Log is never emailed   |
| When Log is full | Log is emailed with log is full  |
| Hourly           | Log is sent every hour   |
| Daily            | Log is sent every day. Select the <b>Time</b> that you want the log to be sent.                          |
| Weekly           | Log is sent every week. Select both the <b>Day</b> and the <b>Time</b> that you want the log to be sent. |

5-7 Config File

This function allows you to save the router's configuration as backup, or retrieve the configuration file you saved before turning the setting back.

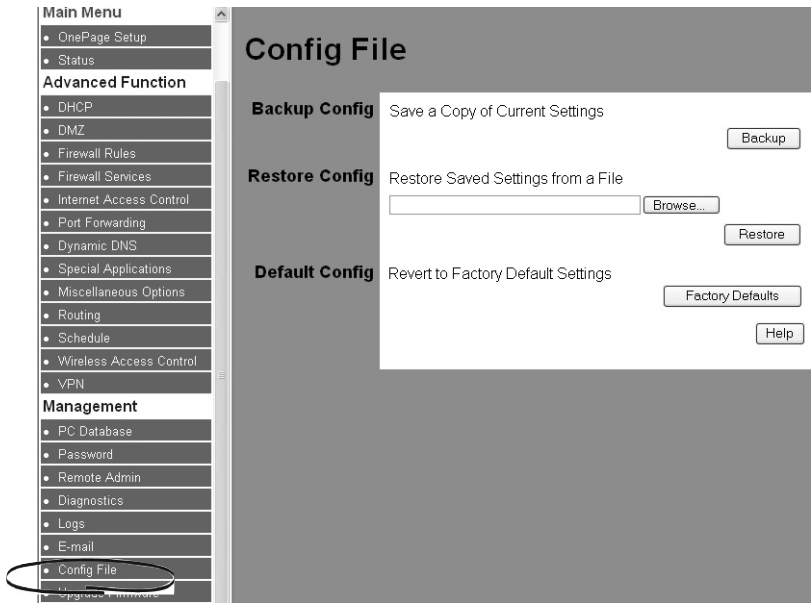


Figure 38. Backup & Restore Configuration

- **Backup Config :** Click the “**Backup**” button to save the current configuration as a backup file. You will be asked where you want to store the file on your local computer.
- **Restore Config:** Enter the path of the configuration file you saved on the PC. You can choose “**Browsing**” to view the folders and select the file. Click “**Restore**” to retrieve it.
- **Default Config:** Click the “**Factory Defaults**” button to restore the router to the default configuration. **Note**, all you existing configuration will be lost.

## 5-8 Upgrade Firmware

This setting page allows you to upgrade to the latest version of firmware to keep your router up-to-date. Before you upgrade the firmware, you have to get the latest firmware and save it on the PC you use to configure the router.

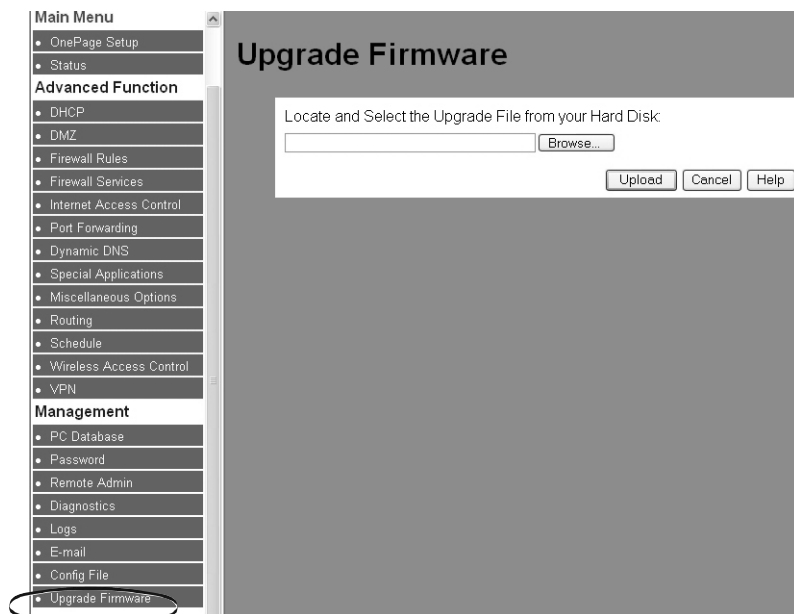


Figure 39. Upgrade Firmware Page

- **Select a file to upgrade:** Enter the path of the latest firmware you saved on the PC. You can choose “**Browsing**” to view the folders and select the firmware.
- **Upload:** After you enter or select the path, click “**Upload**” to proceed to the firmware upgrade process. Please note, do not power off the router during the firmware upgrade.

## Chapter 6.0: Trouble Shooting

This chapter provides solutions to problems you may encounter during installation and operation of your router.

### Hardware

Q: The Power LED is off.

- Check the power cable is properly connected to the router, the power adapter and the socket.

Q: The LAN Link LED is off.

- Check the computer, hub or switch is properly connected to the router.
- Check the computer's Ethernet card is properly installed.
- Check the router and the computer are on the same network segment. If you are not sure, initiate the DHCP function (4-1) and set your computer to obtain an IP address automatically (3-3).
- Check the computer is using an IP address in the range of 192.168.0.2 ~ 192.168.0.254 and is therefore compatible with the router's default IP address of 192.168.0.1 (3-3). Check also the Subnet Mask is set to 255.255.255.0

Q: The STATUS LED stays lit.

- The STATUS LED should light up when the device is first powered up to indicate it is checking for proper operation. After a few seconds, the LED should go off. If it stays lit, the device is experiencing a problem. Please contact your dealer.

Q: Why can't I configure the router?

- First, check whether the router is properly installed or not, it include the LAN and WAN connections, and all devices' power.
- Next, check the IP configuration of your PC:

**For Windows 95,98 users:** run Winipcfg.exe or Winipcfg from Run on the Start menu. If there is no IP address involved, click **Release All** and then click **Renew All** to get IP address.

**For Windows NT 4.0 users:** run Ipconfig.exe or Ipconfig from Run on the Start menu. Ensure that your PC and the router are on the same network segment. If you are not sure, initiate the DHCP function, let the PC get the IP address automatically.

Ensure that your PC is using an IP Address within the range 192.168.0.2 to 192.168.0.254 and thus compatible with the router default IP address of 192.168.0.1

Finally, use Ping command in MS-DOS mode to verify the network connection:

Ping 127.0.0.1 to check the TCP/IP stack of your computer

Ping gateway IP (Default: 192.168.0.1) to check the internal link of network.

If you're not able to get to the web configuration screen for the router, make sure that you remove any proxy setting within your Internet browser, or remove the dial-up settings within your browser.

Q: What can I do if I have forgotten the password for router?

- You have to reset router back to factory default setting by pushing the Reset button over 3 seconds, and refer to the instructions in the user's manual to reconfigure the settings.

Q: I cannot access my ISP's home page, why?

- Some ISPs, such as @Home, require their host name be specifically configured into your computer before you can surf their local web pages. If you are unable to access your ISP's home page, enter your ISP's Domain Name into the OnePage Setup (3-3) to enable all computers in your LAN to access it. If you only want to allow computers to access these home pages, open the TCP/IP Properties window (2-4) on these computers, click open the **"DNS Configuration"** tab and enter your ISP's Domain Name in the **"Domain Name Search Suffix"** location.

### Client Side (Computers)

Q: I can't browse in the internet via the router

- Check the LAN Link/ACT LED on the front panel is lit to indicate proper connection between the computer and the router. Check if both ends of the network cable are properly connected.
- Check that TCP/IP is setup on your computer (2-4). Run "winipcfg" under Windows 95/98 prompt MS-DOS or run "Ipconfig" under Windows NT prompt DOS. Check that the computer's IP Address is in the range of 192.168.0.2 ~ 192.168.0.254 and the Subnet Mask is 255.255.255.0. If you are using a fixed IP address, check also the Default Gateway IP Address and DNS address in **"More"**.

Q: I get a time out error when I enter a URL or IP address.

- Check if other computers work. If they do, ensure the computer's IP settings are correct (IP Address, Subnet Mask, Gateway IP Address and DNS) (4-7).

## Appendix A: Frequently Asked Questions

Q: What is the maximum number of IP Addresses the router can support?

- The router can support up to 253 IP Addresses in the range of 192.168.0.2~192.168.0.254.

Q: Where should the router be installed on the network?

- In a typical environment, the router should be installed between the ISP and your LAN. Connect the router to the phone jack which supplies the ADSL signal, and connect your PCs to the RJ45 jack on the LAN side.

Q: Does the router support IPX or AppleTalk?

- No. The router was designed to provide a multiple user LAN with shared internet access and supports only the TCP/IP Protocol. If your Novell or Apple system is configured with TCP/IP, the router can support them.

Q: Does the router support 100Mb Ethernet?

- Yes, the router supports both 10Mb & 100Mb Ethernet on the LAN side.

Q: What is "NAT" and what is it used for?

- The Network Address Translation (NAT) Protocol translates multiple IP Addresses on a private LAN into a single public IP Address that is accessible to the internet. NAT not only provides the basis for multiple IP Address sharing but also adds to the LAN's security since the multiple IP Addresses of LAN computers are never transmitted directly to the internet.

Q: I cannot access my ISP's home page, why?

- Some ISPs, such as @Home, require their host name be specifically configured into your computer before you can surf their local web pages. If you are unable to access your ISP's home page, enter your ISP's Domain Name into the OnePage Setup (3-3) to enable all computers in your LAN to access it. If you only want to allow computers to access these home pages, open the TCP/IP Properties window (2-4) on these computers, click open the "DNS Configuration" tab and enter your ISP's Domain Name in the "Domain Name Search Suffix" location.

Q: How can a router share a single user account to multiple users?

- The router combines the following technologies to enable this function. NAT (Network address translation): NAT is a technology which can create a private network domain behind a public IP. It is usually used as a firewall. It can also be used when there are not enough IP. DHCP (Dynamic host configuration protocol): DHCP is a protocol to assign IP to internal computers automatically. It can save a lot of IP configuration. This protocol is supported by Windows 95/NT, Mac OS, and many other popular OS. DNS (Domain name service): DNS is a protocol of translating Domain Name to IP address that internet host can handle. Addressing system using Domain name, like www.yahoo.com, is easier to use than IP address, 204.71.177.70.

Q: What operating systems does the router series support?

- The router uses standard TCP/IP protocol, it can be operated as long as you have TCP/IP protocol installed in your operating system (For example: Win9x, Windows NT, Windows 2000 etc.)

Q: Can I use multiple E-mail accounts if I use my router?

- Yes, you can. Some people think having one internet account mean that they can have only one E-mail account. However, E-mail is set by mailbox accounts and different to the account you use to connect to your ISP. If you want more E-mail accounts, you can contact with your ISP or you can browse the internet to apply for a free E-mail account.

Q: Can Internet users access LAN computers?

- The router uses NAT to router all in/out packets. All external users can only see the IP of the router but cannot access LAN computers. The LAN computers are well protected with the router's natural firewall.

Q: When should I use DMZ host?

- Enable DMZ host when you want to have a unrestricted communication between your PC and the internet, for example, playing an internet game (i.e. Ages of Empire) or having a multimedia conference (i.e. NetMeeting).

# Appendix B: Technical Specifications

## Standards Compliance

ADSL G.dmt for 8Mbps downstream & 640Kbps upstream  
ADSL G.lite for 1.5Mbps downstream & 512Kbps upstream  
IEEE 802.3 10/100BASE-T/TX  
IEEE 802.11g Wireless  
IEEE 802.11b Wireless

## Interface

One ADSL interface RJ-11 connector WAN  
Four 10/100Mbps auto-sensing Ethernet RJ-45 connectors

## Management

Web-based UI Management

## LED Display

Power  
Status  
Wireless Link/Activity  
Link/Activity for both ADSL and LAN port(s)

## Environment

Operation Temperature: 0°C ~ 45 °C (32°F ~ 113 °F)  
Storage Temperature: -20°C ~ 60 °C (-4°F ~ 140 °F)  
Humidity: 0 ~ 90% non-condensing

## Dimension

125 x 195 x 35 mm

## Power

External, DC 15V, 1A

## Mounting

Desktop  
Wall-mounting